# KUWAIT TURKISH
# PARTICIPATION BANK INC.

# SUMMARY OF ANTI–MONEY LAUNDERING AND COMBATING FINANCE OF TERRORISM POLICY

---

# Table of Contents

# 1. INTRODUCTION

## 1.1 Nature and Purpose of the Policy

1.1.2 Having a prestigious and trustworthy position, Kuwait Turkish Participation Banks (KTPB, the Bank) is aware of the risks that are inherent in the activities it undertakes, including money laundering (ML) and terrorism financing (TF) risks and their possible implications on its functioning and reputation. Concordantly, with its decisive attitudes on preventing the utilization of its products and services for money laundering and financing of terrorism (AML/CFT) activities and conformance with the local and international AML/CFT standards, the Bank gives great importance to combatting money laundering and financing of terrorism. The Bank also considers it as an important element for compliance with the international system.

1.1.3 The purpose of this Anti-Money Laundering and Combating Financing of Terrorism Policy ("the AML/CFT Policy" or "the Policy") is to outline and reiterate the general principles and guidelines to be embraced and effectively implemented by KTKB to prevent its and any of its branches and subsidiaries from being misused for money laundering or terrorist financing and to outline the framework for regulatory compliance with regards to AML/CFT requirements and obligations.

1.1.4. This Policy therefore reflects the requirements and obligations imposed by the legislations and regulations and is meant to serve as a policy that is to underpin branches' and subsidiaries' AML/CFT policies, procedures and controls.

## 1.2. Objectives of the Policy

Within the framework of this Policy, the Banks aims to;

a. Preserve the elements of respect and trust of the brand, Kuwait Turkish Participation Bank Inc.

b. Ensure that AML/CFT policies and procedures of the Bank comply with the laws and regulations

c. Prevent the Bank from being abused for money laundering and financing of terrorism

d. Have training facilities to inform employees about legal obligations and related principles

e. Evaluate the customers, transactions and services with risk- based approach and develop rules and responsibilities to minimize the potential AML/CFT risk

f. Preserve the customer quality by abiding the KYC principles

# 2. SCOPE

Scope of this Policy covers all employees of Head Office, local and foreign branches, KTPB banking subsidiaries and non-banking subsidiaries to the extent that applicable local laws and regulations permit. Where the AML/CFT requirements in the host country differ from those in Turkey, subsidiaries will apply the higher of the two standards, to the extent that the law of the host country permits so. If the legislation of the relevant country does not allow the implementation of the measures within the scope of the compliance program, the FCIB is notified and additional measures are taken.

**Approval, Revision and Updates**

iv.2.1. This policy shall take effect on the date of the Board approval and it shall continue to be effective until replaced by revised guidelines or is suspended by the BOD.

iv.2.2. The subsequent changes and updates to come as well, will take effect after the approval of the Board as well.

iv.2.3. The policy shall be reviewed at least every two years at by the compliance unit to ensure that it is in line with the industry leading practices and caters for other applicable changes/guidelines issued by any regulatory changes and necessary updates shall be made.

iv.2.4. Amendments to the policy may be made as a result of one or a combination of the following reasons:

a. Changes in laws or regulations;

b. Changes in functions and activities of KTPB;

c. Changes in business processes;

d. Changes in the organizational structure of KTPB;

e. Changes in job roles, duties, and descriptions;

f. Any other change, where the management deems necessary to update KTPB's policies.

## 3. COMPLIANCE OFFICER AND COMPLIANCE UNIT

In order to establish the determined standards in national and international level to the KTPB Head Office, branches and subsidiaries, to follow up the legal arrangements, to take the necessary steps ensuring conformance with current regulations, to arrange training programs to inform the staff about proceeds of crime and finance of terrorism, compliance officer and assistant compliance officer are assigned and the compliance unit is established.

The compliance officer will be directly reporting to one or more BOD members to whom the Board of Directors handed over its responsibilities within the framework of the related legislation although the ultimate responsibility will remain on the KTPB Board of Directors.

In this regard, key responsibilities of compliance officer are as follows;

a. To make the necessary studies for the compliance of the Bank with laws and regulations and to provide the coordination and communication with FCIB.

b. To prepare the Banks' policies and procedures, to review them on regular basis and submit the policies to the approval of the Board of Directors.

c. To develop AML/CFT risk management policy and to execute the risk management activities.

d. To form monitoring and control policies and execute the related activities.

e. To submit the studies on training programs about laundering proceeds of crime and financing of terrorism to the approval of the Board of Directors and to ensure effective implementation of the approved training program.

f. To evaluate the information and findings obtained through researches that he/she has carried out to the extent of his/her power and the possibilities regarding possibly suspicious transactions which were forwarded or detected by his/her initiative and to report the transactions which he/she considered to be suspicious to FCIB

g. To take the necessary measures for ensuring the confidentiality of the suspicious transaction reports and other relevant matters.

h. To regularly keep the information and statistics on internal audit and training activities and send them to the FCIB within the indicated period.

i. To submit periodic/regular reports to the Board of Directors and senior management reflecting the extant of Bank compliance on applicable AML/CFT requirements.

j. To provide guidance, support and advice to branches, departments and subsidiaries on AML/CFT queries.

k. To monitor changes in the legal and regulatory requirements on regarding AML/CFT and share the changes to the relevant function(s) within the Bank.

l. To prepare the unit's own standard procedures manual for the monitoring of transactions and business relationships, the handling and investigation of alerts and suspicions, and clearly determining the division of work and levels of powers among the unit staff.

m. To raise any concerns with the status of compliance that warrant senior management's attention or intervention.

The compliance officer may transfer some or all of his/her duties and authorities to the assistant compliance officer, explicitly and in writing. This kind of authority transfer does not remove the responsibility of the compliance officer in this field.

The compliance officer and compliance unit personnel have the authority to request additional information related to its task, to demand, investigate and search all the related documents, to apply the KTPB staffs' opinions and if necessary to alert the management to take the necessary precautions.

## 4. THE IMPORTANCE OF THIS POLICY BY THE MEMBERS OF KTPB

The KTPB staff should;

4.1. Prevent the use of the Banks' products and services for money laundering and financing of terrorism activities.

4.2. Report the suspicious transactions to the compliance officer within the framework of the legal arrangements and take the necessary actions.

4.3. Abide the legal arrangements about the money laundering and financing of terrorism.

KTKB staff shall be notified about the policy and subsequent changes to this policy. Notification can be made through the procedures permitted by regulations and through electronic media such as intranet, extranet, e-mail or other appropriate methods.

In adhering to this Policy, as with every aspect of its business, KTPB expects that its employees will conduct themselves in accordance with the highest ethical standards. KTPB also expects its employees to conduct business in accordance with applicable money laundering laws. KTPB employees shall not knowingly provide advice or other assistance to individuals who attempt to violate or avoid anti-money laundering and combating finance of terrorism laws or this Policy.

Money laundering laws apply not only to criminals who try to launder their illicit funds, but also to financial institutions and their employees who participate in those transactions, if the employees know that the property is criminally derived. "Knowledge" includes the concepts of "willful blindness" and "conscious avoidance of knowledge." Thus, employees of a financial institution whose suspicions are aroused, but who then deliberately fails to make further inquiries, wishing to remain ignorant, may be considered under the law to have the requisite "knowledge". KTPB employees who suspect money-laundering and financing terrorism activities should refer the matter to appropriate personnel as directed by policies and procedures. Failure to adhere to this Policy may subject KTPB employees to disciplinary action up to and including termination of employment. Violations of anti- money laundering and combating finance of terrorism laws also may subject KTPB employees to imprisonment and, together with KTPB, to fines, forfeiture of assets, and other serious punishment.

KTPB personnel should never hesitate to ask question or report an incident concerning suspicious activity. If an employee becomes aware of a situation in which he/she believes KTPB has been used for money laundering and financing terrorism, or if he/she feels he/she is being pressured or being asked to compromise his/her values, it is his/her responsibility to communicate this event to the compliance officer. It is important for an employee to know that he/she will not be disciplined, lose his/her job, or be retaliated against in any way for asking questions or voicing events about the Policy and related legal obligations, as long as he/she is acting in good faith. Good faith does not mean that he/she has to be right about the issuing question, but it does mean that he/she believes he/she is providing truthful information.

The details and the application procedures of the issues mentioned in this Policy are explained in the AML/CFT procedures.

## 5. AML/CFT PROGRAM

The AML/CFT program in KTPB includes but not limited to the following key elements:

**Commitment**

There should be full commitment from the BOD and the senior management to comply with applicable legal and regulatory requirements related to AML/CFT and sanctions compliance.

All employees are obliged to read this Policy as mandatory and agrees to comply therewith.

**Dedicated AML/CFT Personnel(s)**

The senior management should appoint dedicated and independent personnel(s) responsible to handle AML and CFT compliance matters.

**Implementation of Policy, Procedures, Risk Assessment, Processes & Controls**

The senior management should provide maximum support to compliance unit in implementing the AML and CFT Policy, procedures, risk assessment, processes and controls across the Bank in order to comply with applicable AML/CFT and sanctions compliance requirements.

**Systems**

The senior management should ensure that proper technology systems and proper tools are in place to comply with the applicable requirements.

**AML/CFT Compliance Reporting**

It is the responsibility of the compliance officer to keep the BOD and the senior management abreast of the key issues along with compliance status update through reporting at an assigned frequency or as deemed appropriate.

**Independent Testing & Auditing**

Compliance unit will remain subject to the independent testing and auditing to be conducted by various independent parties including internal/external auditors and the regulatory inspectors.

**Training & Awareness**

The Training Department should ensure that AML/CFT, sanctions related training and awareness sessions are arranged on an ongoing basis to keep all employees abreast of current regulations and practices.

In order to execute the above program, the compliance unit has created and implemented the AML/CFT procedures which are consistent with the requirement of this Policy, local legal and regulatory Instructions in this regard. Furthermore, each function within the Bank is responsible to ensure applicable AML/CFT requirements are duly incorporated into their operational procedures and hence provides complete clarity to the concerned employees.

## 6. KNOW YOUR CUSTOMER PRINCIPLE (KYC)

It is necessary to keep financial and operational honesty, and accordingly to protect the corporate image of KTPB from possible damages by taking all serious steps to prevent KTPB banking network from being used to launder money and finance terrorism.

The principle ‘Know Your Customer’ means KTPB being sufficiently informed about the clients and their activities and developing policies and procedures in order to obtain such data. Additionally, KYC policy

aims to provide awareness about unusual transaction activities or activities inconsistent with the known business of customers.

As part of KYC principle, necessary precautions in the context of applicable regulations and the AML/CFT policies and procedures shall be taken while establishing permanent business relation and executing the client's intended transaction in the following areas:

a. Obtaining sufficient information on the purpose and nature of the intended transaction,
b. Customer identification,
c. Identification of those acting for the benefit of others,
d. Control of the authenticity of documents subject to verification,
e. Customer identification in subsequent transactions,
f. Determining whether the transactions are made on behalf of a third party and identification of those acting on behalf of others,
g. Determining the beneficial owner,
h. Taking necessary measures against customers, activities and transactions that require special attention,
i. Monitoring the client and his/her activities while the business relationship continues,
j. Taking measures against technological risks,
k. Reliance on third party
l. Rejection of transaction and termination of business relationship,
m. Correspondent relationship,
n. Wire transfers,
o. Relationship with risky countries,
p. Applying simplified measures,
r. Applying enhanced measures.

## 7. CUSTOMER IDENTIFICATION

"The Customer" the source of the suspicious transaction, is the basic point in laundering proceeds of crime and combating finance of terrorism. Thus, it is vital to identify customers for the combat against illegal proceeds from crime.

The basic preliminary condition for the Bank to establish a permanent business relation with and execute transactions for a customer is to verify the identity of that customer on a timely and accurate basis. Customer identification shall be carried out via the processes of receiving, determining, controlling and confirming the data.

The identity of a customer shall be verified in order to check the identity details of that customer and of any person acting on behalf of him or real beneficiary of him and confirm the veracity of such details subject to the applicable legislation:

7.1. irrespective of any amount where a permanent business relation is established

7.2. irrespective of any amount whenever there is a suspicion as to the veracity of any customer identity verified before

7.3. irrespective of any amount in circumstances where a suspicious transaction should be reported

7.4. whenever the transaction amount, or the aggregate amount of more than one transaction linked to each other exceed the threshold defined in the applicable legislation, necessary measures shall be taken in order to detect the beneficial owner of the transaction.

7.5. Permanent business relationship can also be established by using remote identification methods, to the extent permitted by the regulations, or by identification through notarized power of attorney.

7.6. When establishing permanent business relationship, information on the purpose and intended nature of the business relationship shall be received.

7.7. As a general rule, a business relationship should never be established or an account should never be opened until the identity of a potential customer is satisfactorily established. If a potential customer refuses to produce any of the requested identity information, the relationship should not be established. Likewise, if requested follow-up information is not forthcoming, any relationship already begun should be terminated.

# 8. CUSTOMER DUE DILIGENCE (CDD) STANDARDS

The Bank will conduct Customer Due Diligence (CDD) to capture KYC information when a new relationship is established. Furthermore, Enhanced Due Diligence (EDD) will be conduct on all customers flagged as high-risk customers as per the AML/CFT Risk Assessment as summarily explained below:

## 8.1 CUSTOMER DUE DILIGENCE (CDD)

Due Diligence at minimum will cover the following as minimum standards either at the account opening stage or at transaction level:

a. Purpose and nature of relationship,
b. Customer Identification and verification measures using reliable source documents, data or information,
c. Linked persons identification and verification measures using reliable source documents, data or information,

d. Identification of beneficial owner and its identity verification using reliable source documents, data or information,
e. Collection of customer KYC information,
f. Declaration that he is sole beneficiary for the account,
g. Name screening on customer and linked persons,
h. Additional information including information on the source of funds as deemed appropriate,
i. Approval by the relevant authority as per the DOA,
j. Business monitoring of account,

Updating of KYC information as per the risk profile of the customer

## 8.2 SIMPLIFIED DUE DILIGENCE (SDD)

The Bank may consider applying simplified measures in terms of customer due diligence in the following situations, consistent with the results of the risk assessment study provided the overall risk rating is low;

a. Transactions between financial institutions themselves,
b. Transactions in which the customers of the obliged parties excluding financial institutions are banks,
c. Transactions in which the customer is a public administration or a quasi-public professional organization,
d. The transactions where customer is an international organization or an embassy or a consulate located in Turkey,
e. Transactions regarding mass customer acceptance within the scope of salary payment,
f. Transactions regarding pension contracts, pension plans and life insurance contracts,
g. Transactions related to salary payments of employees of agencies of international organizations located in Turkey or embassies and consulates,
h. Transactions in which the customer is the company whose shares are listed on the stock exchanges,
i. Transactions relating to the prepaid cards,
j. Obliged parties conducting transactions particularly in electronic environments.

The Simplified Due Diligence (SDD) measures in this regard should be consistent with risk factors as specified in the AML regulations and includes but not limited to the followings:

a. The ability to verify the customer identity and the ultimate beneficiary after establishment of the business relationship,

b. Update the customer data at longer intervals than those specified for the standard usual due diligence measures,

c. Adopting simplified and periodic monitoring and verification,

d. No specific binding or commitment to collect detailed information or taking specific actions to understand the purpose and nature of the business relationship, in that it is sufficient to understand the objective and nature of this relationship in light of the type of the transactions or existing business relationships.

KTPB does not apply simplified measures in cases where money laundering or terrorist financing risks might occur due to the transaction and shall take into account that the transaction is possibly a suspicious transaction.

## 9. ENHANCED DUE DILIGENCE (EDD)

KTPB shall apply, in proportion to the identified risk, one or more or all of the following enhanced measures for transactions within the scope of the headings of Transactions Requiring Special Attention, Taking Measures Against Technological Risks, Relations with Risky Countries and for high risk situations it has identified in the framework of risk-based approach.

Obtaining additional information on the customer and updating more regularly the identification data of customer and beneficial owner,

9.1.1. Obtaining additional information on the intended nature of the business relationship,

9.1.2. Obtaining information, to the extent possible, on the source of the asset subject to transaction and source of funds of the customer,

9.1.3. Obtaining information on the reasons for the transaction

9.1.4. Obtaining approval of senior manager to commence or continue business relationship or carry out transaction,

9.1.5. Conducting enhanced monitoring of the business relationship by increasing the number and frequency of the controls applied and by selecting the patterns of transactions that needs further examination,

9.1.6 Requiring that in the establishment of permanent relationship the first financial transaction is carried out through another financial institution subject to customer due diligence principles.

## 10. KYC DATA UPDATING

Relevant Business Units are responsible to update customer data, profiles and documentation in accordance with the requirements defined in operational procedures. The Business will conduct customer KYC update exercises regarding customer information and data, including measures to ensure

that the Bank obtains valid permissible replacements for expired official customer identity documents as per the below schedule:

| No. | Customer Risk Type | KYC Update Frequency |
|---|---|---|
| 1. | Customers classified as “High Risk” based on the AML/CFT Risk Assessment | Annually |
| 2. | Customers classified as “Medium Risk” based on the AML/CFT Risk Assessment | 2 years |
| 3. | Customers classified as “Low Risk” based on the AML/CFT Risk Assessment | 3 years |

# 11. RISK MANAGEMENT FRAMEWORK

KTPB pays a particular attention to risk management in order to define, rank, monitor asses and decrease the risks that it may face in relation to potential misuse of its banking services for the purpose of money laundering and financing terrorism. The definition and ongoing monitoring of risky areas, risky lines of business and risky transactions and also establishing enhanced due diligence and client acceptance procedures help the KTPB to prevent the use of its products and services for money laundering and financing of terrorism purposes.

By Risk management activities, KTPB aims at defining, ranking, monitoring, assessing and minimizing the risks that the Bank may face. Risk management covers the internal measures and rules of practice in relation to ‘Know Your Customer’ whose headlines are given below. The details of such internal measures and rules of practice are specified in the AML/CFT procedures.

## 11.1. RISK LIMITATION

Risk limitation is the maximum level of risk that the Bank is willing and prepared to accept during the normal course of business. The Bank in principle consider money laundering and terrorist financing risk very seriously and will take all reasonable steps to mitigate the risk of breaches within the Bank operations. Bank will ensure that appropriate remedial action is taken to address instances of non-compliance with its obligations and that it will refuse to establish/continue relationship or process a transaction where perceived money laundering, terrorist financing or sanctions busting risk is large or unmanageable.

The Bank part of its commitment will comply with the followings as minimum:

a. It will not open or keep anonymous accounts or accounts in fictitious names.

b. It will not deal with a person who is found to be engaged in any activity that could be potential sources for money laundering like casinos, online lotteries, lotto draws, betting transactions etc.

c. It will not deal with a sanctioned person.

d. It will not establish any new business relationship in a sanctioned jurisdiction in line with the applicable sanctions program.

e. It will not deal with a Shell Bank or a bank which allows a shell bank to use its accounts.

f. It will not deal with an entity where identity of the Ultimate Beneficial Owner (UBO) is not identified and verified.

g. It will not deal with a person engaged in activities which may damage the Bank reputation such as illegal distribution arms, munitions, drugs, narcotics, human trafficking, adult entertainment, gambling etc.

h. It will not establish a business relationship unless the customer, which includes beneficial owners, shareholders, persons holding Powers of Attorney, authorized signatories, has been subjected to sanctions screening.

## 11.2. RISK ASSESSMENT AND RISK BASED APPROACH

The KTPB, within the context of the anti-money laundering and combating finance of terrorism risk management defines the country risk, customer risk and transaction risk concepts, then grades the customers, transactions and products/services according to their risk potential and classifies them. As a result of this classification, in the next step, the KTPB creates procedures for monitoring transactions and customers, pays great attention to get the information about the source of income of these customers by requesting additional documents and confirming them.

Risk Management Activities implemented by KTPB include at least the following activities:

11.2.1. Developing risk defining, rating, classifying and assessing methods based on customer risk, product/service risk and country risk,

11.2.2. Rating and classifying services, transactions and customers depending on risks,

11.2.3. Developing proper operational and control rules for ensuring monitoring and controlling risky customers, transactions or services; taking necessary measures in order to mitigate the risks; reporting in a way that warns related units; carrying out the transaction with the approval of senior management and controlling it when necessary,

11.2.4. Questioning retrospectively the coherency and effectiveness of risk defining and assessing methods and risk rating and classifying methods depending upon sample events or previous transactions, reassessing and updating them according to achieved results and new conditions,

11.2.5. Carrying out required development works through pursuing recommendations, principles, standards and guidelines introduced by local legislation and international organizations related to issues under the scope of risk,

11.2.6. Reporting risk monitoring and assessing results regularly to the executive board.

The money laundering and financing terrorism related risks the Bank may face due to the Bank's customers, their activities and transactions, are classified into three main categories in the light of legislation;

a. Customer Risk
b. Service/Product Risk
c. Country Risk

On the ground of monitoring and control, KTPB's customers, product/services and transactions are ranked as low, medium or high risk; risk profiles of customers in terms of money laundering and financing terrorism are prepared as low, medium or high, based on their business past, activities, financial capacity, accounts and country of business and location and other indicators; and they are subjected to monitoring activities.

Customers designated as high risk will be subject to EDD measures including continuous monitoring and an annual KYC update.

## 12. HIGH RISK CUSTOMERS

Before establishing a business relationship with those taking place in the following sectors and professions, a particular attention is paid and the customer identities as well as sector information are provided with diligence and their accounts are monitored with care. In that regard, some of the key high-risk customer segments are as follows:

a. Non-profit organizations
b. Politically Exposed Persons (PEP's)
c. Cross border correspondent banks/shell banks
d. Exchange companies
e. Customers originating from sanctioned and high-risk jurisdictions
f. Nonresident customer
g. Embassies/Consulates
h. Gold, precious stones and precious metal dealers
i. Arms and ammunition dealers/contractors
j. Car Dealers

## 13. HIGH RISK PRODUCTS AND SERVICES

Transaction that its source activity cannot be identified and those which cannot be related to the client's area of business, generally cash transactions, products made out for the bearer and customer funds and

transactions generated from digital fund transfers are monitored with enhanced due diligence procedures.

13.1. The following products are assessed as high-risk category products and services:

13.1.2 Electronic fund transfers

13.1.3. Collection of personal cheques drawn on foreign banks

13.1.4**.** Systems enabling non-face to face transactions

## 14. RELATONS WITH RISKY COUNTRIES

KTPB pays special attention to business relationships and transactions with the natural and legal persons, unincorporated organizations and the citizens located in risky countries and obtains information about the purpose and the nature of the transactions, as far as possible, which have no apparent reasonable legitimate and economic purpose and to record them.

14.1. The following countries and regions, the customers based on or related to those countries and regions are monitored as country-based high-risk customers:

14.1.2. The countries existing in the black and grey lists declared by FATF,

14.1.3. The countries given in the list of 'Risky Countries', declared by the relevant Ministry,

14.1.4 The countries put under sanction by either UN, EU or OFAC for their policies and practices in relation to money laundering and financing of terrorism,

14.1.5 Countries deemed as risky in international regulations in relation to money laundering and financing of terrorism.

## 15. TERMINATION OF BUSINESS RELATIONSHIP AND REJECTION OF TRANSACTION

Bank will refuse to establish a new relationship or terminate an existing relationship with customers or customer segments completely or partially and not conduct the transaction which is requested on the grounds of:

15.1. Bank inability to conduct due diligence on the customer,

15.1.1. Customer failure to provide KYC information as required by the Bank, whether at onboarding stage or while updating such information during the course of the relationship,

15.1.2. Bank is unable to identify and verify the identity of the customer or the ultimate beneficiary,

15.1.3. Customer reluctance to cooperate with the Bank on queries raised to satisfy internal requirements,

15.1.4. Customer failure to comply with the applicable account Terms & Conditions,

15.1.5. Unacceptable or unmanageable money laundering risk.

KTPB shall also assess whether the situations specified above are suspicious transactions or not.

## 16. MONITORING AND CONTROL ACTIVITIES

The purpose of KTPB's monitoring and controlling is to protect the Bank against risks and to monitor and control whether the operations are carried out in accordance with the relevant regulations.

Monitoring and control activities shall be established and applied on a risk-based approach. In this respect, certain monitoring and control methods that suit the nature and level of risks associated with the Bank customers, transactions and services shall be developed and effectively implemented. On the ground of monitoring and control activities, KTPB ensures that the staff carrying out such activities shall have access to in-house information sources.

16.1. Monitoring and controlling carried internally include the following activities:

16.1.1. Monitoring and controlling the customers and transactions in the high-risk group,

16.1.2. Monitoring and controlling transactions conducted with risky countries,

16.1.3. Monitoring and controlling complex and unusual transactions,

16.1.4. The Bank's control of consistency of the amount determined by the Bank according to its risk policy with the customer profile, through sampling method,

16.1.5. Monitoring and controlling linked transactions which, when handled together, exceed the amount requiring customer identification,

16.1.6. Control of customer related information and documents which are required to be kept in electronically or in written form and the information required to be placed in wire transfer messages, completing the missing information and documents and updating them,

16.1.7. During the business relationship, ongoing monitoring whether the transaction conducted by the customer is consistent with information regarding business, risk profile and fund resources of the customer,

16.1.8. Control of the transactions carried out through using systems enabling the performance of non-face-to-face transactions,

16.1.9. Risk based control of services that may become prone to misuse due to newly introduced products and technological developments.

16.2. In that regard, the activities of central monitoring and control are carried by the compliance unit. In doing so and determining the suspicious transactions, technological means are to be used and benefited from.

16.3. As for auditing and controlling the efficiency and appropriateness of the activities conducted on the basis of applicable regulations and the compliance program, it is carried out by the Internal Audit Department and the deficiencies determined are communicated to the compliance officer. The data containing information on works made toward this end shall be reported to the FCIB by the compliance officer.

## 17. SANCTON COMPLIANCE

The Bank is fully committed to comply with all legal and regulatory requirements relating to sanctions compliance. Furthermore, Bank will ensure that no new relationship is established with a sanctioned person under UNSC lists, OFAC, EU, local lists, etc.

Furthermore, bank where possible will consider terminating the relationship with sanctioned customers listed by OFAC or any lists adopted by KTPB to the extent possible.

In case of domestic banking transfers, it is the responsibility of the issuing bank to verify that the name of the one requesting the transfer is not included in the names listed in the freezing lists and not to deal with him, while it is the responsibility of the receiving bank to verify that the name of the beneficiary is not included the names listed in the freezing lists and not to deal with him.

## 18. TRAINING AND AWARENESS PROGRAM

Within the context of the relevant national and international regulations about money laundering and terrorism financing, and that of KTPB policies, KTPB's all existing and new employees, including BOD and executive management, are included in an on-going training and awareness raising program. When invited, the KTPB staff should attend these programs and should read all the documents and materials published for educational and training purposes.

The purpose of this on-going training and awareness raising program is to ensure the compliance of KTPB with the obligations imposed by the relevant regulations, to create a corporate culture by increasing the sense of responsibility of staff on policy and procedures of institution and on risk-based approach and to update the knowledge of the staff.

18.1. The training and awareness raising activities conducted by KTPB in that regard shall be carried out in the light of the following principles:

18.1.1 The training program shall be prepared by the compliance unit and its efficiency is to be supervised by the compliance unit.

18.1.2 Annually training program is approved by the Board of Directors.

18.1.3 KTPB may use visual and listening materials and computer-based training programs which operate on internet, intranet or extranet, in a way that will extend the training available across the whole Bank.

18.1.4 Trainings are organized by Training Department, upon the request of the compliance officer.

18.1.5 In-class trainings are given by the compliance unit or through outsourcing.

18.1.6 Training may be run as online seminar training.

18.1.7 Training activities are run through a program and a plan and at least cover the following subjects.

a. Laundering proceeds of crime end terrorist financing
b. The stages and methods of laundering proceeds of crime and case studies on this subject
c. Legislation regarding prevention of laundering proceeds of crime and terrorist financing
d. Risky areas
e. Institutional policies and procedures
f. Principles relating to customer identification
g. Principles relating to suspicious transaction reporting
h. The procedure for suspicious transaction report
i. Obligation of retaining and submitting
j. Obligation of providing information and documents
k. Sanctions to be implemented in violation of obligations
l. The international regulations on combating laundering and terrorist financing
m. The potential effect on the Bank, its employees and customers, of any breaches of the AML/CFT laws or regulations
n. Customer identification
o. The detection and prevention of money laundering and terrorist financing
p. The detection of unusual or suspicious activities
q. Money laundering and terrorist financing typologies and trends
r. The procedures for making an internal suspicious transaction report
s. Customer due diligence measures with respect to establishing new business relationships with customers
t. Sanction programs

The information and statistics on training activities shall be reported to FCIB in line with the schedules determined by the relevant regulations.

## 19. INTERNAL AUDIT ACTIVITIES

The purpose of internal audit activities carried by the internal audit departments is to give assurance to the Board regarding efficiency and sufficiency of whole compliance program.

KTPB ensures, annually and on a risk based approach, the investigation and control of the issue of whether the AML/CFT policies and procedures formed in line with the relevant legislation, risk management, monitoring and controlling activities and the training programs are sufficient and efficient and the issue of sufficiency and efficiency of risk policy of the Bank and whether the transactions are carried out in compliance with the relevant regulations and the Bank's AML/CFT Policy and procedures.

19.1. Internal audit carried within this framework covers the following activities:

19.1.1. The deficiencies, mistakes and abuses determined as the result of internal audit and the opinions and proposals for prevention of reappearance of them shall be reported to the BOD.

19.1.2. While determining the scope of audit, the faults detected during the monitoring and controlling activities and the customers, services and transactions containing risk shall be included within the scope of audit.

19.1.3. While determining the units and transactions to be audited, the business size and business volumes of the Bank shall be taken into consideration. In this scope, unit and transaction in the quantity and characteristics of which can represent the whole transactions carried out by KTPB shall be ensured to be audited.

19.1.4. The statistics regarding the works carried out in the scope of internal audit activities shall be reported to FCIB in line with the schedules determined by the relevant regulations.

## 20. SUSPICIOUS TRANSACTION REPORTING

Where there is any information, suspicion or reasonable grounds to suspect that the asset, which is subject to the transactions carried out or attempted to be carried out within or through the Bank, has been acquired through illegal ways or used for illegal purposes and is used, in this scope, for terrorist activities or by terrorist organizations, terrorists or those who finance terrorism necessary investigation to the extent permitted by the applicable means shall be carried out and any transaction concluded to be suspicious shall be reported to the FCIB within such term and subject to such conditions defined in the relevant regulations by compliance officer of the Bank. Suspicious transactions shall be reported to FCIB within ten workdays starting from the date when the suspicion occurred.

20.1. The Bank shall not disclose any information that the suspicious transaction has been or will be reported to anyone including the parties of the transaction, except for the information provided for the examiners assigned for supervision of obligations and for the courts during trial.

20.2. KTPB is fully committed to develop an open and transparent working environment wherein employees are encouraged to speak up and report suspected or known violations of internal requirements without any fear of reprisal.

20.3. All employees are obliged to report immediately all instances of suspected, perceived or known violations of this Policy and by escalating the concern to compliance unit through banking system, email or other appropriate means. The Bank reaffirms that all such referrals provided in good faith and in

accordance with the requirements of the Law will protect employees from criminal, civil and administrative liability in all cases.

20.4. After the additional investigation and assessment of the compliance officer, if the activity is to be found suspicious, it is reported to FCIB by additional information and supporting documents.

20.5. Maximum care and diligence shall be paid by all concerned parties that are either involved in or aware of the process subject to the relevant regulations that suspicious transaction reporting as well as the internal reporting within the Bank shall be kept confidential and safe, and the parties involved in the process shall be duly protected.

## 21. RECORD KEEPING

The Bank shall retain documents, books and records, identification documents and records kept in all forms regarding its transactions and obligations for eight years starting from the drawn-up date, the last record date, the last transaction date respectively and submit them when requested. The starting date of retaining period relating to documents on customer identification concerning the accounts within obliged parties is the date when the account has been closed.

Documents and records of suspicious transactions reports made to FCIB or internal reports made to the compliance officer, documents attached to reports, the written reasons relating to suspicious transactions decided not to be reported by compliance officers are all in the scope of obligation of retaining and submitting.

## 22. POLICY OWNER

This Policy has been prepared by KTPB Compliance Officer taking local regulations into account and approved by Board of Directors of KTPB.

## 23. EFFECTIVENESS

This policy shall take effect on the date of the Board approval. The subsequent changes and updates to come as well, will take effect after the approval of the Board as well.